Audit Report

OFFICE OF THE INSPECTOR GENERAL

CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE

Report Number 93-056

February 19, 1993

Department of Defense

The following acronyms are used in this report.

7CG.....Air Force 7th Communications Group
ADPE.....Automated Data Processing Equipment
ASD(C3I).....Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
DASD(IS).....Deputy Assistant Secretary of Defense (Information Systems)
DTSA.....Defense Technology Security Administration
LAN.....Local Area Network
MDW.....U.S. Army Military District of Washington
MOU.....Memorandum of Understanding
NAVAIR.....Naval Air Systems Command
SPA.....Software Publishers Association
USAISC.....U.S. Army Information Systems Command

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

February 19, 1993

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE)
ASSISTANT SECRETARY OF THE NAVY (FINANCIAL MANAGEMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
INSPECTOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Controls Over Copyrighted Computer Software (Report No. 93-056)

This is our final report on controls over copyrighted computer software. The report identifies a significant level of unauthorized use of copyrighted software on computers throughout the Department of Defense.

A draft of this report was issued to the addressees for comment on September 30, 1992. Comments from the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) were received on November 25, 1992, and from the Department of the Army on October 19, 1992.

The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) concurred with the conditions described in the report but nonconcurred with the recommendations to alleviate the conditions on the premise that existing laws and Federal regulations require copyrighted software to be controlled. In view of the pervasion of the condition disclosed by the audit and for the specific reasons provided in the Audit Response section in Part II of the report, we request that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) reconsider the need for corrective action in this matter and provide additional comments in response to this final report.

The Army concurred with the finding and the recommendations in the draft report. The Departments of the Navy and Air Force did not reply to the draft report. While not required, the Navy and Air Force are invited to comment on the final report.

DoD Directive 7650.3 requires that all audit recommendations be resolved promptly. Recommendations are subject to resolution in accordance with the Directive in the event of nonconcurrence

or failure to comment. Therefore, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) must provide final comments on the unresolved recommendations within 60 days of the date of this report.

In view of the potential existence of the conditions discussed in this report throughout the Department, the distribution has been expanded, as shown in Appendix F, beyond that normally afforded our reports. Should recipients desire additional copies for distribution to subordinate activities, they can be obtained by contacting the office designated on the Table of Contents.

The courtesies extended to the audit staff are appreciated. If you have any questions on this audit, please contact Mr. Harrell D. Spoons, the Program Director, at (703) 692-2846 (DSN 222-2846) or Mr. Marvin L. Peek, the Project Manager, at (703) 692-2939 DSN (222-2939).

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

AUDIT REPORT NO. 93-056 **February 19, 1993**
(Project No. 2RF-5004)

CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE

EXECUTIVE SUMMARY

Introduction. Copyrighted computer software programs are used on as many as 377,500 microcomputers throughout the DoD. DoD does not maintain records on the number of software programs on hand, but the proliferation of computers within DoD suggests that millions of software programs may be in use. Federal copyright law grants copyright owners exclusive rights to duplicate or distribute the programs. Although software vendors attempt to control unauthorized use of their products through licensing agreements that invoke the protection available under copyright statutes, compliance with licensing agreements relies on the integrity of the software user.

Objective. The audit objective was to determine whether policies and procedures for controlling and using computer software programs within the DoD were adequate to ensure compliance with licensing agreements and copyrights. We also evaluated applicable internal controls.

Audit Results. The audit showed that 51 percent of the 1,022 computers tested had copyrighted software programs installed without documentation to prove that the software had been legally acquired. Unauthorized use of copyrighted computer software contravenes Federal laws and denies software vendors their rightful revenues.

Internal Controls. We found material weaknesses in the internal controls designed to monitor the installation and accountability of copyrighted computer software programs. The controls we assessed are described in Part I of the report, and the finding provides details on the weaknesses.

Potential Benefits of Audit. No monetary benefits are associated with the recommendations in this report. Implementation of the recommendations will strengthen controls over the use of copyrighted software and reduce the risk of copyright infringement in the DoD. A summary of benefits resulting from this audit is in Appendix D.

Recommendations. We recommended that the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) issue better guidance, requiring all DoD Components to establish and enforce controls over the use and accountability of copyrighted computer software. No recommendations were directed to the

Military Departments. However, because the conditions disclosed by the audit were prevalent throughout the DoD, the report was addressed to the Military Departments to provide an opportunity to comment on the results of the audit.

Management Comments. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) concurred with the finding, but nonconcurred with the recommendations, stating that existing laws and regulations are already in place. We believe the Assistant Secretary needs to provide leadership by issuing stronger and more explicit guidance on the need for better internal controls.

The Army concurred with the finding and the recommendations; the Navy and the Air Force did not provide comments. The complete texts of managements' comments are in Part IV. The Assistant Secretary of Defense (Command, Control, Communications and Intelligence) should provide comments on the unresolved issues within 60 days of the date of this report.

TABLE OF CONTENTS

This report was prepared by the Readiness and Operational Support Directorate, Office of the Assistant Inspector General for Auditing, DoD. Copies of the report can be obtained from the Secondary Reports Distribution Unit, Audit Planning and Technical Support Directorate (703) 614-6303 (DSN 224-6303).

PART I - INTRODUCTION

Background

At the end of FY 1991, DoD activities reported having about 377,500 automated data processing equipment (ADPE) systems on hand that cost less than $15,000 each. Only summary records were reported for ADPE systems costing less than $50,000; therefore, the audit assumed that ADPE systems costing less than $15,000 were primarily microcomputers. DoD does not maintain an overall inventory of computer software, and no reliable estimates were available indicating the cost to purchase software for microcomputers within DoD. However, since microcomputer users rely almost exclusively on commercially developed, off-the-shelf software programs and since multiple software programs are common on each microcomputer, it is reasonable to assume that millions of commercially developed software programs are installed on microcomputers in DoD. Because of the wide variance in the cost of popular commercial software programs, we could make no meaningful estimate concerning the total cost of software installed on DoD microcomputers.

Software vendors attempt to control unauthorized use of their products through license agreements that invoke the protection available under Federal copyright statutes. The specific license agreement for each software product is explained in documentation accompanying the system disks that enable the user to install and operate software programs on a computer. Although the wording may differ slightly, license agreements specify that each software program purchased is to be used on one computer at a time. In some instances, an activity may purchase a "site license" or a license to use a software program on a local area network (LAN) of computers. Such licenses permit an activity to use the covered software program on the number of computers stated in the agreement. Most vendors have chosen not to incorporate built-in controls to disable software when it is copied; therefore, compliance with license agreements relies on the integrity of the software user.

U.S.C., title 17, section 106, gives owners of copyrights the exclusive rights to reproduce, distribute, or make derivative works of their material. Section 504 of the statute states that a copyright infringer is liable for actual damages to a copyright owner or statutory damages up to $100,000. The Defense Federal Acquisition Regulation Supplement, paragraph 252.227-7013, also provides provisions for commercial software purchased by DoD activities. In summary, the provisions state that ownership of the software remains with the contractor (i.e., copyright holder), and the Government has the right to use software in the computer for which the software was acquired.

Organizations within the computer software industry, such as the Software Publishers Association (SPA), have heightened public awareness of software copyright requirements. The SPA is fighting software piracy through a three-way approach of litigation, education, and public relations. Settlements reached with companies accused of software piracy range into the hundreds of thousands of dollars. The audit did not identify any litigation involving misuse of copyrighted software at any of the activities visited; however, U.S.C., title 28, section 1498, states that owners of commercial software copyrights can take action against the Federal Government for copyright infringement.

Objectives

The overall objective of the audit was to determine whether policies and procedures for controlling and using computer software programs within DoD were in accordance with licensing agreements and copyrights. Specifically, we determined whether the DoD activities audited were complying with copyright laws and licensing agreements, and we evaluated internal controls over copyrighted software.

Scope

The audit included a review of each Military Department's guidance on controls over copyrighted software and the implementing procedures in use at the subordinate commands and activities audited. We physically examined a judgmental sample of computers at each activity to determine whether the software installed on microcomputers was supported by documentation showing that it had been legally acquired. We examined 1,022 computers in 22 activities within the Military Departments. The sample was limited to IBM[1]-compatible computers. At the time of the audit, over 90 percent of the microcomputers within DoD were IBM-compatible. Records pertaining to software procurement, accountability, and inventories were examined when such records were maintained. We also reviewed audit reports and management reports related to software management that were issued from FY 1987 through FY 1991 by the Military Department audit agencies and other organizations responsible for controls over software.

This program audit was made from December 1991 through June 1992 in accordance with auditing standards issued by the Comptroller General of the United States as implemented by the Inspector General, DoD, and accordingly included such tests of internal controls as were considered necessary. Activities visited or contacted are listed in Appendix E.

---

1 IBM is a registered trademark of the International Business Machines Corporation.

Internal Controls

The audit identified material internal control weaknesses as defined by Public Law 97-255, Office of Management and Budget Circular A-123, and DoD Directive 5010.38. Controls either had not been established or were not adequate to ensure compliance with software licensing agreements. Furthermore, some activities did not maintain records of software procurement or accountability that were adequate to verify that computer software was legally acquired. Details on the internal controls we reviewed and the weaknesses we found are described in the Finding. All the recommendations in this report, if implemented, will correct the weaknesses. No quantifiable monetary benefits will be realized by implementing the recommendations; however, increased emphasis on compliance with software licensing agreements should help prevent violations of copyright laws, possible litigation against the Government, and resulting fines and penalties. A copy of this report will be provided to the senior officials responsible for internal controls within the Office of the Secretary of Defense and the Army, Navy, and Air Force.

Prior Audits and Other Reviews

Inspector General, DoD, Audit Report No. 92-092, "Alleged Misuse of 'SGT Security' Commercial Software," May 15, 1992, evaluated the merits of an allegation that the Air Force 7th Communications Group illegally copied and used "SGT Security" software. The allegation could not be substantiated. The report contained no recommendations.

Inspector General, DoD, Audit Report No. 92-134, "Controls Over Copyrighted Computer Software at the Defense Technology Security Administration," (DTSA) September 9, 1992, showed that DTSA had violated licensing agreements by installing copyrighted computer software that had not been purchased and had not maintained adequate documentation for other software installed. The report recommended that DTSA identify and remove unauthorized software and establish internal controls over the acquisition and use of copyrighted software. Management concurred with the finding and recommendations and initiated corrective actions.

The Army Audit Agency issued five installation reports as a result of one multilocation audit. The audit found that 41 percent of the computers sampled had undocumented commercial software installed. The audit also found that commercial software was not properly accounted for or controlled and that policies governing the control and use of software installed on Army-owned computers had not been established. Two summary reports were issued in 1989 as a result of that audit. Two other audits that included Army activities in Europe and Army Reserve activities had similar findings. Details on the Army Audit Agency reports are in Appendix A. We found similar deficiencies

at Army organizations we audited. Audit results at one of the installations, Headquarters, Information Systems Command, for which a report had been issued by the Army Audit Agency, are shown in the Finding of this report.

Although no Air Force-wide audits of controls over computer software have been conducted, the Air Force Audit Agency issued 33 reports on individual installations from FY 1987 through FY 1991. Of the 33 reports, 28 showed that software had been installed without documentation to show that it had been legally acquired. The reports recommended removing unauthorized software, maintaining and reconciling software inventory records, and performing random reviews to ensure only authorized software is installed. The Air Force Audit Agency performed follow-up audits for 4 of the 33 reports. Three of the follow-up reports showed that corrective actions had not been taken. A summary of the reports is provided in Appendix B. We audited two activities at Dover Air Force Base, Delaware, for which the Air Force Audit Agency had issued reports. The 436th Logistics Support Squadron had implemented the audit recommendations, and all computers tested at that activity had documentation supporting the software that was installed. The 436th Military Airlift Wing had not implemented the audit recommendations.

Other Matters of Interest

Demonstration software. Software manufacturers sometimes provide individuals or organizations software for use on a trial basis. The capabilities of the software and the terms and conditions for use vary. Some demonstration software is fully functional only for a limited time. Other demonstration software is fully functional, and software vendors may ask that it be returned if it is not purchased. In other cases, the software may be provided free. Irrespective of the terms or conditions of use, it is important that the use and particularly the return of demonstration software is documented. As part of this audit, we reviewed allegations by a software manufacturer that the Air Force 7th Communications Group (7CG) failed to return the original copy of a demonstration software program and made illegal copies of the program.[2] The allegation was not substantiated; however, the 7CG had not implemented procedures to document the receipt and return of demonstration software. Although such procedures may not have prevented the allegation, documentation of the return of the software would have appreciably reduced the efforts expended in determining the validity of the allegation.

Shareware. Shareware is user-supported software or "try before you buy" software that is normally distributed free of charge through computer bulletin boards or advertisements in computer magazines. Shareware authors encourage users to give

2 Report No. 92-092, "Alleged Misuse of 'SGT Security' Software," May 15, 1992.

copies to others for evaluation as a way of advertising the product. The language used in shareware copyright notices has caused confusion about the need to pay for such software. For example, some copyright notices "encourage" users to register and remit a specific fee, and terms like "contribution" or "donation" are used to describe payment. Regardless of the language used, Code of Federal Regulations, title 37, states that Government entities that continue using shareware programs after the trial period must pay for such use. Here again, documentation is important to show the use or disposition of the software to avoid perceptions of or actual misuse.

This page was left out of original document

PART II - FINDING AND RECOMMENDATIONS

CONTROLS OVER COPYRIGHTED SOFTWARE

Unauthorized software had been installed on 51 percent of 1,022 computers tested. This condition existed because controls to ensure compliance with computer software licensing agreements and copyright laws were either ineffective or nonexistent and because of management indifference. Unauthorized copying, dissemination, and use of copyrighted computer software in DoD contravenes Federal law, denies copyright owners their rightful revenues, and exposes the DoD to potential litigation and public discredit.

DISCUSSION OF DETAILS

Guidance

DoD. DoD Instruction 7920.5, "Management of End User Computing," March 1, 1989, states that it is DoD policy to enforce the licensing provisions of commercial software. The Instruction tasks DoD Component heads with ensuring compliance with the terms and conditions of copyright and licensing agreements. Additionally, "Defense Ethics," a guide for DoD employees published in January 1989 by the Inspector General, DoD, states:

> Vendor software may not be reproduced for distribution, other than to authorized Government agencies, according to the terms and conditions of the contract. If you violate copyright laws and other conditions of a software licensing agreement, you are acting on your own accord, and disciplinary action may be taken against you.

Army. Army Regulation 25-1, "Army Information Resources Management Program," November 18, 1988, states that proprietary software must be protected by the user/accountable individual from unauthorized use, abuse, or duplication. Although formal property book accountability is not required, software is to be controlled as a durable, receipted item. However, the Regulation does not specify that software should be traced to a specific computer, and the audit showed that receipts had been prepared for multiple copies of software without identification of the computers on which the software was authorized to be installed.

Five of the seven Army activities audited had issued local guidance emphasizing the need to comply with software licensing agreements and copyright laws. Two major command headquarters that we audited, U.S. Army Information Systems Command (USAISC) and U.S. Army Military District of Washington (MDW), issued regulations requiring that annual inventories of software be made for accountability and control and that original software diskettes be maintained by authorized users for auditing purposes. The regulations also required that each software user sign a Memorandum of Understanding (MOU) (see Appendix C) that summarized the provisions of the software licensing agreements. However, the audit showed that the MOUs were not being used by the organizations audited within those two command headquarters. To be effective, controls must be implemented and enforced.

Navy and Marine Corps. At the time of the audit, no Navy-wide instructions regarding controls over copyrighted computer software had been issued. However, a Secretary of the Navy instruction was being prepared that would address controls over copyrighted software. Among the Navy's major commands, only the Naval Air Systems Command (NAVAIR) had issued instructions governing the use of copyrighted software. NAVAIR Instruction 5239.1, "Software Duplication Policy," December 20, 1985, states that it is NAVAIR policy not to make copies of copyrighted software unless authorized in writing by the copyright owner. During the audit, the Naval Facilities Engineering Command published a similar instruction, but only three of the four Navy field activities audited had issued guidance that emphasized the importance of complying with software licensing agreements. However, none of the instructions addressed how software should be accounted for or controlled.

The Marine Corps Small Computer Systems Security Manual (the Manual), May 23, 1990, states that making unauthorized copies of software is a violation of copyright laws and that employees are subject to indictment and conviction if found guilty. Further, the Manual recommends conducting periodic software inventories and requiring users to sign a document acknowledging they are prohibited from making unauthorized copies. Furthermore, "White Letter" No. 4-90, "Computer Viruses," June 29, 1990, issued by the Commandant of the Marine Corps, prohibits the use of copied or pirated software.

Air Force. Air Force Regulation 700-26, "Management of Small Computers," December 15, 1988, summarizes copyright laws, stating that copying commercially purchased software without a license agreement is illegal. The Regulation requires that an inventory of the software installed on each computer be maintained. Although the Regulation requires software accountability at the user level, the audit showed that the requirement for inventories was not enforced at the activities audited. For example, guidance issued by Headquarters, Air Force Logistics Command, required that a "software control log" be established for each computer system. However, the guidance to

establish accountability was not followed. Furthermore, only four of the seven Air Force activities audited had issued implementing guidance.

Review of Software on Computers

The audit showed that unauthorized software had been installed on computers at each of the 22 Military Department activities audited. This condition existed even though each activity was given prior notice of the purpose and date of the audit. Each activity had ample opportunity to remove unauthorized software from their computers, and some commands had directed such removal. The results of the audit tests are shown Tables 1., 2., and 3. below.

Table 1. Results of Computers Tested - Army

Activity	Computers Tested	Computers with Undocumented Software	Number of Undocumented Software Programs
Headquarters, Army Staff	53	28	78
Headquarters, Information Systems Command, Fort Huachuca	45	16*	33*
Headquarters, Military District of Washington, Fort McNair	30	13	23
Headquarters, Army Depot System Command	19	7	12
Fort Belvoir	76	61	136
Fort Bragg	68	46	199
Letterkenny Army Depot	62	34	84
Totals	353	205	565

* On August 26, 1992, USAISC informed us that documentation had been located for all but 12 undocumented software programs we found during our audit. We did not verify the information since it was provided after our visit to USAISC.

Table 2. Results of Computers Tested - Navy and Marine Corps

Activity	Computers Tested	Computers with Undocumented Software	Number of Undocumented Software Programs
Navy			
Headquarters, Naval Air Systems Command	31	16	57
Headquarters, Naval Facilities Engineering Command	37	19	58
Headquarters, Naval Supply Systems Command	31	9	15
Naval Command, Control, and Ocean Surveillance Center; Research, Development, Test, and Evaluation Division	44	30	79
Naval Supply Center, San Diego	42	31	85
Norfolk Naval Shipyard	71	33	56
Public Works Center, San Diego	62	24	47
Marine Corps			
Central Design and Program Activity, Quantico	48	8	10
Totals	366	170	407

Table 3. Results of Computers Tested - Air Force

Activity	Computers Tested	Computers with Undocumented Software	Number of Undocumented Software Programs
Headquarters, Air Staff	60	31	109
Headquarters, Air Force Logistics Command	42	25	59
Headquarters, Tactical Air Command	52	14	24
1st Tactical Fighter Wing, Langley Air Force Base	30	30	116
7th Communications Group	35	4	6
2750th Airbase Wing, Wright-Patterson Air Force Base	41	29	64
Dover Air Force Base	43	17	31
Totals	303	150	409

None of the officials at the audited activities could provide evidence to show that a total of 1,381 copyrighted software programs installed on 525 (51 percent) of the 1,022 computers tested had been legally acquired. We estimated the retail value of the unauthorized software programs at about $227,000.

Undocumented software. Computer users offered various reasons why undocumented software was installed on the computers tested. From the reasons cited, it was evident that the problem stemmed from ineffective or nonexistent controls and a lack of management emphasis on compliance with licensing agreements. For example, computer users claimed they were unaware of certain software programs installed on their computers, that the software was already installed on computers when they were assigned, that software documentation had been lost, or that they were unaware of or did not understand copyright restrictions.

Controls. The relatively low cost of software programs intended for use on microcomputers, the need to make backup copies of system disks, and the ease of illegally duplicating disks create a daunting control challenge. However, effective controls are essential to ensure compliance with software licensing agreements and Federal copyright statutes. The following examples show that controls ranged from reasonably effective to nonexistent among the activities audited.

o The Training Management Section, 436th Logistics Support Squadron, Dover Air Force Base, developed effective procedures to control and account for all software installed on its computers. A custodian maintained an inventory of all software installed on the 15 computers within the Training Section. He also maintained the original diskettes, by computer serial number, in a central location. No undocumented software was found on the eight computers tested at the Training Section. The Training Section had been included in a software audit by the Air Force Audit Agency in 1990 and had implemented recommendations resulting from that audit.

o The Resource Management Directorate, Headquarters, U.S. Army Depot System Command, had developed procedures to account for software and to inform users of their responsibilities. An inventory of the software installed on each computer was maintained with the machines. Additionally, original diskettes, bar coded to identify the computer on which the software was installed, were kept locked in a storage cabinet. Supervisors, managers, and computer users were required to attend an annual Automation Security Briefing, reminding them of local policies and of software copyright restrictions. Those personnel were required to sign a form acknowledging their responsibilities and their understanding of policies and procedures for automation security and controls over computer software. Each individual was also given a reference copy of the policies and procedures. Only 1 unauthorized software program was installed on the 10 computers tested.

o After being notified of the audit, the 7th Communications Group (7CG) instructed computer users to remove all software that could not be supported by purchase documentation. The 7CG also provided each user and the Computer Systems Security Officer a list of the software authorized on each computer. Each user was to maintain the original software and documentation. These procedures to control and account for software were established in a 7CG instruction published during the audit. The audit tested 35 computers and found 6 unauthorized software programs.

o At one Army unit, the software on the computers had not been inventoried and was not identified on receipts at the user level. Users could not provide reasons why unauthorized software was installed on their computers. During our exit briefing, the unit commander stated most users probably assumed

that all software was "owned" by the Army and could be used and copied freely. The audit tested 10 of 27 computers and found 76 unauthorized software programs.

o An Air Force squadron branch had issued an Operating Instruction that stated, "It is generally illegal to make several copies of one original software product then run the copies on different systems." However, the branch chief stated he understood that only one copy of each software package in use needed to be purchased. He indicated that individual software programs that had been purchased were copied to the majority of computers in the branch. The audit tested 8 of 14 computers and found 44 unauthorized software programs installed.

Documentation. Records at some activities were not adequate to show that software had been legally acquired. For audit purposes, the original copyrighted software diskettes, site licenses, receipts, and accreditation packages showing specific software had been authorized were accepted as evidence of legal ownership. When documentation was available to establish ownership of a software program, the audit treated all copies of the software as authorized, up to the quantity for which ownership had been established, even though records did not identify the specific computer on which the software was installed. We questioned 421 software programs because no records were available to show where the software was authorized to be installed, but we did not count those programs as unauthorized. However, since copyrighted software ordinarily may be used on only one computer at a time, knowledge of where each copy of a software program is installed is necessary to ensure compliance with the licensing agreement. The absence of such records highlights the lack of adequate internal controls over the use of copyrighted software.

o We tested 24 computers at one Army Headquarters Staff activity and were unable to determine whether 132 software programs installed were authorized, because accreditation packages with documentation for authorized software by computer were incomplete and frequently could not be matched to a specific computer.

o Software and supporting documentation for one Pentagon-based Air Force Headquarters Staff activity was maintained by a custodian located at Bolling Air Force Base. Because the custodian kept software for about 300 users, the volume of material required that the software and documentation be stored at three separate locations. None of the software was identifiable to a specific computer or user. The custodian kept the software documentation because users complained that it took up too much space.

At some of the activities audited, personnel claimed that software may have been purchased, but diskettes and manuals, which provide evidence of software ownership, had been lost. For

example, when undocumented software was found at one unit at Fort Bragg, the Commander stated that software documentation was lost during the buildup for Operation Desert Shield and the deployment for Operation Desert Storm.

The audit showed that there were fewer instances of unauthorized software when computers were operated on a LAN. However, even though LANs eliminate the need for installing most software programs on individual computers, the following examples show that controls are still needed to guard against unauthorized software.

o Computers at one section of the Navy Public Works Center, San Diego, were connected to a LAN. Only two designated personnel were authorized to install or remove software. Software approved for installation on the LAN was stored in a central location and could be easily inventoried. If additional software was approved, it was maintained with the specific user for whom it had been authorized. The audit tested 17 computers and found only 3 unauthorized software programs.

o The Marine Corps Central Design and Programming Activity's computers were connected to a LAN. Most of the activity's authorized software was installed on the LAN rather than on the hard drives of individual computers. The audit tested 48 computers and found only 10 unauthorized software programs.

Management emphasis. Computer security officers interviewed during the audit reported that efforts to control copyrighted computer software were hampered by a lack of command emphasis on the importance of complying with copyright laws and licensing agreements. The problem is illustrated by the following examples.

o The Chief of Staff at one Army activity stated that because software has minimal value, the command could not afford to expend the hours needed to account for every software program. In his opinion, most software should be considered a consumable item without a requirement to account for it.

o The computer security officer at one Navy command credited the audit with helping the command's senior management to recognize that a problem existed. After the audit, the command began an extensive review of software needs and developed plans to purchase the necessary software to ensure compliance with software licensing agreements.

o At one Air Force activity where unauthorized software was installed on computers, personnel reported that they were frequently required to respond to senior management taskings using specific software programs even though the software had not

been purchased. The deputy director of the activity stated that he had verbally advised senior management of this problem, but the practice continued.

o Within 1 section of an Air Force squadron, we tested 12 of 20 computers and found 21 unauthorized software programs. The squadron commander knew that unauthorized copies of software programs in excess of the quantities purchased had been installed on the squadron computers. He stated that due to insufficient funds, the required number of copies of the software could not be purchased, but that the software programs were needed for the squadron's mission and the mission came first.

Conclusions

The audit results cannot be statistically projected because the sample was judgmental; however, the results are sufficient to show that licensing agreements for copyrighted computer software were ignored at all levels of command in each Military Department. Taken together with similar results reported by the Army and Air Force Audit Agencies (see Appendixes A and B), the audits present compelling evidence that abuse of software licensing agreements has been and remains commonplace throughout DoD. Most significantly, the audit showed that leaders and managers have not only acquiesced in the continuing abuse of software licensing agreements, but that they have directed actions that required violation of Federal copyright statutes. Disregard of Federal law under the guise of expediency signals an unacceptable breakdown in integrity and ethical behavior among those who are responsible.

The public has a right to expect honest and fair treatment when dealing with the DoD. It is incumbent on all public servants, both military and civilian, that the highest standards of ethical behavior and personal integrity be maintained in all official matters. Senior leaders must demand and enforce the highest standards of conduct, and potential copyright infringers must be assured that improper acts will be dealt with appropriately.

Formal controls over copyrighted computer software and formal procedures for implementing the requisite controls are necessary to ensure that leaders, managers, and computer users know and apply needed safeguards to preclude copyright infringement. The needed guidance has not been issued at all activities. Furthermore, the audit showed that, with rare exception, existing guidance was generally ignored by the activities audited. Controls need not be onerous; management enforcement is the key to effectiveness. Unauthorized software should be prohibited. In order to negate any future allegation of copyright infringement, proof of legal possession of copyrighted software and a record to show on which computer the software is installed should be retained for as long as the software is used.

RECOMMENDATIONS FOR CORRECTIVE ACTION

We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issue guidance requiring DoD Components to:

1. Inform all personnel of copyrighted computer software licensing agreements and of the potential consequences for copyright infringement.

2. Prohibit the possession or use of unauthorized copyrighted computer software, and administer disciplinary action for any circumvention.

3. Establish controls to ensure that proof of legal possession of copyrighted computer software is retained for as long as the software is used.

4. Establish procedures to identify copyrighted computer software that is authorized to be installed on each computer.

MANAGEMENT COMMENTS AND AUDIT RESPONSE

Management comments. In responding for the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) the Deputy Assistant Secretary of Defense (Information Systems) (DASD[IS]) concurred with the finding, but nonconcurred with the recommendations. The DASD(IS) also doubted that the majority of the incidents of improperly documented software were the result of willful violations of copyright laws. The complete text of the comments is in Part IV of the report.

The DASD(IS) stated that existing laws and Federal regulations, as cited in the draft report, already have established the requirement to control copyrighted software. Thus, the problem is noncompliance with, rather than a lack of, laws and regulations. The comments suggested noncompliance could be addressed as part of routine IG, DoD, inspections and audits.

The response stated that the problem will get more visibility because the DASD(IS) Information Management Self-Assessment Guide addresses the extent to which DoD Components have implemented internal controls to preclude the unlawful copying of copyrighted software. Also, DASD(IS) officials are evaluating the feasibility of including language regarding copyrighted software in future DoD directives or instructions, but in the interim, they are satisfied with existing policy in DoD Instruction 7920.5, "Management of End User Computing." The Instruction tasks Component heads to "Ensure compliance with the terms and conditions for commercial software use, including copyright and license agreements."

The DASD(IS) suggested minor changes to the draft report section entitled "Prior Audits and Other Reviews," regarding violations on licensing agreements at the Defense Technology Security Administration and corrective actions taken.

Audit response. We agree with the DASD(IS) that the major cause of violations of licensing agreements and copyright laws is noncompliance with existing laws and regulations. However, the audit showed that existing DoD and Military Department guidance was not effective in preventing abuse of copyrighted software licensing agreements. DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I])," February 12, 1992, makes the ASD(C3I) the principal DoD official responsible for establishing software policy and practices. The ASD(C3I) has not promulgated policy guidance stressing the need for all management levels to ensure compliance with software licensing agreements. Given the audit evidence that abuse of software licensing agreements within DoD is commonplace, management's comment that it is "satisfied with existing policy" reinforces the overall impression of management indifference to the abuse of software licensing agreements.

The Software Copyright Protection Act (Public Law 102-561) was signed by the President on October 28, 1992. The Act provides penalties of up to 5 years in prison and fines of up to $250,000 for persons infringing on at least 10 copies of a copyrighted software program or any combination of programs with a retail value greater than $2,500. Had that law been in effect during the audit, referrals to criminal investigative activities would have been necessary. We believe the criminal penalties need to be brought to the attention of all DoD managers and microcomputer users.

Audit recommendations were not addressed to the DoD Components because we believe the ASD (C3I) must lead on this issue. Guidelines directed to the data processing and information management technical communities will not suffice. Our audit recommendations focus on what DoD Components should do to "ensure compliance with the terms and conditions of commercial software use...." as stated in DoD Instruction 7920.5. The recommendations also emphasize the need to establish controls and procedures to identify software authorized to be installed on computers. If these procedures are not established, DoD activities will not be able to determine whether they are in compliance with software licensing agreements, and disciplinary actions cannot be administered for noncompliance.

DASD(IS) personnel provided us a copy of the Information Management Self-Assessment Guide, dated November 25, 1992. The Guide helps implement DoD Instruction 7740.3, which requires DoD activities to conduct periodic reviews of their information management installations. The Guide contains 141 internal control questions on 17 functional areas. Three of the questions relate to controls over copyrighted computer software. While the

Guide is helpful, we believe that three questions on software controls buried in an overall information management guide do not constitute the emphasis senior DoD management should convey to correct the problem.

Changes in the wording of the "Prior Audits and Other Reviews" section were made in the final report based on management's comments. However, our comments regarding corrective actions by the Defense Technology Security Administration (DTSA) (Report No. 92-134) were not changed. Our report stated that DTSA had initiated corrective actions. We did not state that DTSA had taken corrective actions, since we did not verify actions taken after the audit was completed.

We consider management's comments to be nonresponsive because no corrective action is planned. For the reasons cited above and in the details of the conditions, we maintain that the audit recommendations are still valid. However, we have changed the wording of the recommendations from requiring a "DoD Directive" to requiring "guidance," so that management has more flexibility in responding to the need for demonstrating a stronger interest in establishing proper internal controls in this area. We agree that DoD oversight organizations will have an important role in monitoring compliance with those controls, but management should not wait for further reports of noncompliance with the law to take corrective and preventative action. We request that the ASD(C3I) reconsider the matter and provide comments on each recommendation in response to this final report.

Other Comments. The Army concurred with the recommendations. The Navy and the Air Force did not provide comments to the draft report. Should they desire, the Navy and Air Force may respond to this final report.

PART III - ADDITIONAL INFORMATION

This page was left out of original document

APPENDIX A: SUMMARY OF ARMY AUDIT AGENCY REPORTS ON COMPUTER SOFTWARE MANAGEMENT

The U.S. Army Audit Agency conducted three multilocation audits from March 1988 through December 1990, covering the acquisition, use, control, and accountability of commercial software.

One multilocation audit resulted in five installation reports that were consolidated into the two summary audit reports listed below. The problems and suggested corrective actions were also reported in two advisory reports with the same titles.

- Report No. SW 89-209, "Commercial Software Copyrights," May 29, 1989

- Report No. SW 89-208, "Acquisition, Use, and Control of Commercial Software," June 12, 1989

The Army Audit Agency found that:

- Policies and procedures had not been established to prevent, detect, or control unauthorized copying of commercial software.

- Policies and controls were not adequate to ensure that commercial software was properly accounted for and controlled.

- The Army Internal Control Program, as it relates to the acquisition, use, and control of commercial software was not adequate.

Based on a statistical sample:

- 41 percent of the Army-owned "personal" computers had undocumented copies of commercial software valued at $21 million;

- $43 million in software disks and documentation were improperly secured;

- 43 percent of the computers had unapproved shareware and "freeware"; and

- 18 percent of the computers had software acquired by personnel.

The Army Audit Agency found that the planning, justification, and approval process for the acquisition of commercial software and training programs for commercial software users were inadequate. Also, inadequate guidance had been issued for handling lost,

stolen, damaged, or excess software; registering software; and safeguarding software. These areas were not included in the scope of our audit.

The Army Audit Agency recommended that policies and procedures be established to:

- Deal with past potential copyright infringements by identifying undocumented commercial software and establishing a contingent liability.

- Inform users of their responsibilities to honor software copyrights.

- Require periodic reviews of computer hard drives to identify undocumented software.

- Discipline personnel when copyright infringements are identified.

- Physically safeguard software.

- Control shareware, "freeware," and privately owned software.

- Account for commercial software.

- Require annual physical inventories of all software and its documentation, and reconcile inventoried software with quantities recorded in property books.

Report No. SW 89-208 also recommended that the internal control checklists be revised, that guidance be furnished to information managers on their internal control responsibilities related to commercial software, and that a tracking system be developed to identify material weaknesses concerning commercial software.

The Army agreed that software was undocumented. However, based on advice from the Army General Counsel, the Army disagreed with the results of the statistical sample and the need for a contingent liability. The Army issued an Army-wide message in February 1989, directing local organization or installation managers to ensure compliance with copyright policy and to advise and assist customers who may not be familiar with the software copyright laws and agreements.

Two other multilocation audits had similar findings and recommendations:

- Report No. EU 89-309, "Commercial Automation Software U.S. Army, Europe, and Seventh Army," May 1, 1989, states that accountability controls over commercial software, worth about $3.4 million, were not adequate.

- Report No. NE 91-300, "Acquisition, Use, and Maintenance of Automatic Data Processing Equipment and Software, 94th U.S. Army Reserve Command," April 12, 1991, states 89 percent of computers tested at four Army Reserve centers had undocumented software.

This page was left out of original document

APPENDIX B: SUMMARY OF AIR FORCE AUDIT AGENCY REPORTS ON SMALL COMPUTER SOFTWARE MANAGEMENT

The Air Force Audit Agency issued 33 reports from FY 1987 through FY 1991 on small computer software management and 4 follow-up reports. The reports included reviews of 3 major command headquarters (Military Airlift Command; Air Force Communications Command; and U.S. Air Forces, Europe) and 30 bases or activities. The majority of the audit reports identified the following deficiencies.

- Unauthorized copyrighted software was found on computers tested (28 of 33 reports).

- Required software inventories were not maintained on computers tested (23 of 33 reports).

- Excess software was not properly identified and turned in for reutilization (16 of 33 reports).

- Software was not adequately safeguarded (17 of 33 reports).

The recommendations to correct deficiencies varied, but generally stated:

- Remove unauthorized software from Government-owned computers.

- Perform random spot checks of computer hard drives and software inventory records to determine that only authorized software is installed.

- Maintain software inventory records, and reconcile records periodically with original documentation to identify and resolve discrepancies.

- Provide adequate training to accountable personnel to ensure excess software is turned in for redistribution. Perform random spot checks to ensure compliance.

- Make backup master copies of software programs, and store diskettes in acceptable containers and areas.

Only one of the four follow-up reports stated that the deficiencies identified had been corrected. At three activities (Headquarters, Military Airlift Command; Headquarters, Air Force Communications Command; and 375th Military Air Wing), procedures had not been fully implemented to remove unauthorized software from computers.

This page was left out of original document

APPENDIX C: SAMPLE MEMORANDUM OF UNDERSTANDING FOR USERS OF COMMERCIAL SOFTWARE

MEMORANDUM OF UNDERSTANDING
BETWEEN
DEPUTY CHIEF OF STAFF FOR INFORMATION MANAGEMENT
PLANS DIVISION
AND
MDW USERS OF COMMERCIAL SOFTWARE

SUBJECT: Computer Software Protection Policy

1. I recognize that computer software for Government-owned information systems may be licensed for a variety of outside companies. MDW does not own this software or its related documentation. Unless specific permission has been granted by the software licensor, no user has the right to (a) copy or reproduce software (this does not apply to authorized backup copies, (b) copy or reproduce the software package's related documentation, or (c) allow the software to be used simultaneously by another user.

2. I understand that software will only be used in accordance with the software licensing agreement.

3. I understand that if I knowingly make, acquire, or use unauthorized copies of computer software, I may be subject to discipline according to the circumstances.

4. I understand that pursuant to Federal statute, illegal reproduction of commercial software for personal use is subject to civil damages up to $50,000 and criminal penalties to include fines and imprisonment in accordance with Title 17, United States Copyright Code 504 and 506.

5. I have read and understand the software protection policies of AR [Army Regulation] 380-19, paragraph 2-4, and MDW supplement 1 thereto, and will abide by them.

_____
SIGNATURE/DATE

_____
NAME/GRADE

_____
ORGANIZATION/TELEPHONE NO.

This page was left out of original document

APPENDIX D: SUMMARY OF POTENTIAL BENEFITS RESULTING FROM AUDIT

Recommendation Reference	Description of Benefit	Type of Benefit
1.	Compliance and Internal Controls. Ensures all personnel are aware of copyright restrictions and penalties for abuse of licensing agreements.	Nonmonetary
2.	Internal Controls. Eliminates possession and use of unauthorized software.	Nonmonetary
3.	Internal Controls. Requires procedures to account for copyrighted computer software while it is in use.	Nonmonetary
4.	Internal Controls. Requires procedures to preclude unauthorized use of copyrighted computer software.	Nonmonetary

This page was left out of original document

APPENDIX E: ACTIVITIES VISITED OR CONTACTED

Office of the Secretary of Defense

Assistant Secretary of Defense, (Command, Control, Communications, and Intelligence), Washington, DC
Deputy Assistant Secretary of Defense (Management Systems)

Department of the Army

U.S. Army Inspector General Agency, Washington, DC
Deputy Chief of Staff (Logistics), Washington, DC
Deputy Chief of Staff (Plans and Operations), Washington, DC
Director of Information Systems for Command, Control, Communications, and Computers, Washington, DC
U.S. Army Audit Agency, Alexandria, VA
U.S. Army Information Systems Command, Fort Huachuca, AZ
U.S. Army Military District of Washington, Fort McNair, Washington, DC
  Fort Belvoir, VA
U.S. Army Depot System Command, Chambersburg, PA
  Letterkenny Army Depot, Chambersburg, PA
Headquarters, XVIII Airborne Corps and Fort Bragg, NC

Department of the Navy

Naval Information Systems Management Center, Assistant Secretary of the Navy (Research, Development, and Acquisitions), Washington, DC
Naval Air Systems Command, Washington, DC
Naval Sea Systems Command, Washington, DC
  Norfolk Naval Shipyard, Portsmouth, VA
Naval Supply Systems Command, Washington, DC
  Naval Supply Center, San Diego, CA
Naval Facilities Engineering Command, Alexandria, VA
  Navy Public Works Center, San Diego, CA
Naval Audit Service, Arlington, VA
Space and Naval Warfare Systems Command, Washington, DC
  Naval Command, Control, and Ocean Surveillance Center, Research, Development, Test, and Evaluation Division, San Diego, CA
Naval Computer and Telecommunications Command, Washington, DC

APPENDIX E: ACTIVITIES VISITED OR CONTACTED (Cont'd)

Department of the Air Force

Assistant Secretary of the Air Force (Acquisitions), Washington, DC
Judge Advocate General, Air Staff, Washington, DC
Chief of the Air Force Reserve, Washington, DC
Deputy Chief of Staff (Personnel), Washington, DC
Deputy Chief of Staff (Command, Control, Communications and Computers), Washington, DC
Deputy Chief of Staff (Logistics), Washington, DC
Civil Engineer, Air Staff, Washington, DC
Air Force Audit Agency, Washington, DC
Air Force Logistics Command, Wright-Patterson Air Force Base, OH
  2750th Air Base Wing, Wright-Patterson Air Force Base, OH
Tactical Air Command, Langley Air Force Base, VA
  1st Tactical Fighter Wing, Langley Air Force Base, VA
7th Communications Group, Washington, DC
436th Airlift Wing, Air Mobility Command, Dover Air Force Base, DE

Marine Corps

Marine Corps Computer and Telecommunications Activity, Quantico, VA
Marine Corps Central Design and Programming Activity, Quantico, VA

Specified Commands

Headquarters, Forces Command, Fort McPherson, GA

Defense Agencies

Defense Automation Resources Information Center, Defense Information Systems Agency, Alexandria, VA

APPENDIX F: REPORT DISTRIBUTION

Office of the Secretary of Defense

Under Secretary of Defense Acquisition
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
  Director of Defense Information
  Deputy Assistant Secretary of Defense (Information Systems)
Assistant Secretary of Defense (Force Management and Personnel)
Assistant Secretary of Defense (Health Affairs)
Assistant Secretary of Defense (International Security Affairs)
Assistant Secretary of Defense (Legislative Affairs)
Assistant Secretary of Defense (Production and Logistics)
Assistant Secretary of Defense (Program Analysis and Evaluation)
Assistant Secretary of Defense (Public Affairs)
Assistant Secretary of Defense (Reserve Affairs)
Comptroller of the Department of Defense
  Deputy Comptroller (Management Systems)
  Director, Management Improvement
  Deputy Comptroller (Program/Budget)
Director of Defense Procurement
Director, Defense Research and Engineering
  Deputy Director (Test Evaluation)
Director, Operational Test and Evaluation
Assistant to the Secretary of Defense (Atomic Energy)
Assistant to the Secretary of Defense (Intelligence Oversight)
Director, Defense Acquisition Regulations Council
  (OASD[P&L], DASD[P]/DARS)
Assistant to the Secretary of Defense (Intelligence Policy)
Director, Administration and Management

Joint Staff

Director, Joint Staff
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command
Commander in Chief, U.S. Forces Command

Department of the Army

Secretary of the Army
Director of Information Systems for Command, Control, Communications and Computers
Inspector General, Department of the Army
Auditor General, Army Audit Agency

APPENDIX F: REPORT DISTRIBUTION (Cont'd)

Department of the Navy

Secretary of the Navy
Assistant Secretary of the Navy (Financial Management)
Comptroller, Department of the Navy
Assistant Secretary of the Navy (Research, Development, and Acquisitions)
Commandant of the Marine Corps
Auditor General, Naval Audit Service

Department of the Air Force

Secretary of the Air Force
Assistant Secretary of the Air Force (Financial Management and Comptroller)
Deputy Chief of Staff, Command, Control, Communications and Computers
Auditor General, Air Force Audit Agency

Defense Agencies

Director, Defense Advanced Research Projects Agency
Director, Defense Commissary Agency
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Intelligence Agency
Director, Defense Investigative Service
Director, Defense Legal Services Agency
Director, Defense Logistics Agency
Director, Defense Mapping Agency
Director, Defense Nuclear Agency
Director, Defense Security Assistance Agency
Director, National Security Agency Central Security Service
Director, On-Site Inspection Agency
Director, Strategic Defense Initiative Organization

Non-DoD Activities

Office of Management and Budget
U.S. General Accounting Office
National Security and International Affairs Division, Technical Information Center
Software Publishers Association

APPENDIX F: REPORT DISTRIBUTION (Cont'd)

Non-DoD Activities (Cont'd)

Chairman and Ranking Minority Member of Each of the Following Congressional Committees and Subcommittees:

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Committee on the Judiciary
Senate Subcommittee on Patents, Copyrights, and Trademarks, Committee on the Judiciary
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Operations
House Subcommittee on Legislation and National Security, Committee on Government Operations
House Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations
House Committee on the Judiciary
House Subcommittee on Courts, Intellectual Property, and the Administration of Justice, Committee on the Judiciary
House Committee on Science, Space, and Technology
House Subcommittee on Science, Research, and Technology, Committee on Science, Space, and Technology
House Permanent Select Committee on Intelligence
House Subcommittee on Oversight and Evaluation, Permanent Select Committee on Intelligence

This page was left out of original document

PART IV MANAGEMENT COMMENTS

Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

Department of the Army

This page was left out of original document

ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGECE) COMMENTS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-3040

COMMAND CONTROL COMMUNICATIONS AND INTELLIGENCE

NOV 25 1992

MEMORANDUM FOR DIRECTOR, READINESS AND OPERATIONAL SUPPORT DIRECTORATE, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Draft Audit Report on Controls Over Copyrighted Computer Software (DoD Inspector General (DoDIG) Project No. 2RF-5004)

My staff has reviewed the subject draft audit report and circulated it to appropriate Components for comment.

We concur with the findings in the subject draft. The findings cannot be disputed, although we doubt that the majority of the incidents of improperly documented vendor proprietary software are a result of willful violations of copyright laws.

We do not concur with the recommendations. Existing laws and Federal regulations, as cited in the draft report, establish the requirement to control copyrighted software. The problem is not a lack of, but noncompliance with, existing laws and regulations, which could be addressed as part of DoDIG routine inspections and audits.

This problem will get more visibility in the future, because we have included a section in our Information Management Self Assessment Guide that addresses the extent to which Components have implemented internal controls to preclude the unlawful copying of copyrighted software. We are also evaluating the feasibility of including language regarding copyrighted software in future DoD Directives or Instructions; but in the interim, are satisfied with existing policy. DoD Instruction 7920.5, "Management of End User Computing," specifically tasks heads of Components to, "Ensure compliance with the terms and conditions for commercial software use, including copyright and license agreements." DoD 7740.1-G, "Department of Defense ADP Internal Control Guideline", July 1988, has a section on "Specific Microcomputer Control Considerations," which addresses this issue with the question, "Do policies prohibit the use of copyrighted and/or unauthorized software that the activity has not leased or purchased?"

The attachment to this memorandum contains recommended changes to the section on "Prior Audits and Other Reviews" in the Introduction of the draft report.

ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE) COMMENTS (Cont'd)

Should you have any questions regarding this response, my action officer is Tom May, at 703-746-7918.

C Kendall

Cynthia Kendall
Deputy Assistant Secretary of Defense
(Information Systems)

Attachment

Final Report Reference

Draft Audit Report on Controls Over Copyrighted Computer Software (DoD Inspector General (DoDIG) Project No. 2RF-5004)

Page 5, Last paragraph: 3

Change "...DTSA had violated licensing agreements by installing copyrighted computer software that had not been purchased."

To read:"...DTSA had violated licensing agreements by installing copyrighted computer software for which purchase transactions had not been completed or for which adequate documentation could not be provided."

Rationale: The proposed wording provides an overall picture of the results of the DTSA Audit as it is reflected in report number 92-134, dated September 9, 1992. As stated on page 3 of the audit report, DTSA was found to have copyrighted software installed without documentation to show it had been legally acquired. At no time was there any finding that cites evidence of willful violation of the copyright laws. The recommended wording correctly states the findings.

Page 6, Continuation of last paragraph on page 5, last sentence: 3

Change: "Management concurred with the findings and recommendations and initiated corrective actions."

To read: "Management concurred with the recommendations and has taken corrective actions."

Rationale: While DTSA did not take exception to the general thrust of the findings, it did not necessarily concur with the wording of each finding or conclusion. As noted in Mr. Rudman's memorandum of August 14, 1992, DTSA "accepted its [the IG's] recommendations." Mr. Rudman also noted that the IG report does not cite evidence of willful violation of the copyright laws and that DTSA's own internal review did not reveal any such evidence (see pp. 19-20 of report number 92-134). Since Mr. Rudman's memorandum, DTSA has substantially completed implementation of the corrective actions recommended by the IG and the proposed language change reflects this progress.

Attachment

This page was left out of original document

DEPARTMENT OF THE ARMY COMMENTS

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
WASHINGTON, DC 20310-0107

Office, Director of Information Systems for Command, Control, Communications, & Computers

SAIS-IDP (36-2b)

19 Oct 92

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF ~~THE ARMY~~ Defense
~~ATTN: SAIG-PA (Ms. Flanagan),~~ PAF.
~~WASHINGTON DC 20310-1700~~

SUBJECT: Draft Audit Report on Controls Over Copyrighted Computer Software (Project No. 2RF-5004)

1. Reference memorandum, SAIG-PA, 8 Oct 92, SAB, which forwarded for our review the draft DoD audit report.

2. We concur with all recommendations contained in the draft DoD audit report.

3. My point of contact is Mr. Arnold, (703) 614-0559.

FOR THE DIRECTOR:

Linda S. Dean

LINDA S. DEAN
Deputy Director for Policy

CF:
SAIS-ADW

AUDIT TEAM MEMBERS

William F. Thomas, Director, Readiness and Operational Support Directorate
Harrell D. Spoons, Program Director
Marvin L. Peek, Project Manager
John Van Horn, Team Leader
Adrienne Brown, Team Leader
Steve Borushko, Auditor
Lynn Concepcion, Auditor
Lisa Earp, Auditor
Rhonda Carter, Auditor
Nancy C. Cipolla, Editor
Paula D. Stark, Secretary

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Controls Over Copyrighted Computer Software

B. DATE Report Downloaded From the Internet: 05/15/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 05/15/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.